Notice of Allowability	Application No.	Applicant(s)	
	09/896,197	ROELSE, PETRUS LAMBERTUS ADRIAANUS	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/27/2005*.

2. ☒ The allowed claim(s) is/are *2-13 and 15-20*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. Appeal Brief, under 37 CFR 41.37, has been filed. Claims 2-13 and 15-20 have been examined. Examiners amendment has been made for independent claim 13 based on the telephone interview, with Robert M. McDermott, on September 14, 2005.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert M. McDermott, Esq., Reg. No. 41,508 on September 14, 2005.

3. In response to the amendment after notice of appeal filed on August 23, 2005, please replace the examiner's amendment for independent claim 13 as follows:

13. (Currently Amended) A system for cryptographically converting an input data block in to an output data block; the system including:

an input for receiving the input data block;

a storage for storing a predetermined set of at least two permutations associated with an S-box;

a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation; the processor being operative to each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box; ~~and~~

an output for outputting the processed input data block(.) ; and

wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance:

Claims 2-13 and 15-20 are allowed.

Claim 1: Prior art of record neither alone nor in combination teach a method for cryptographically converting an input data block into an output data block that includes selecting a select permutation from a predetermined set of at least two permutations and performing a non-linear substitution operation on the input data block based on the select permutation, *wherein the set of permutation is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.*

Claim 13: Prior art of record neither alone nor in combination teach a system for cryptographically converting an input data block into an output data block. The system

includes a storage for storing a predetermined set of at least two permutations associated with an S-box, a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation, the processor being operative to each time before using the S-box selecting the permutation from the stored set of permutations associated with the S-box, *wherein the set of permutation is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.*

Claim 18: Prior art of record neither alone nor in combination teach a cryptographic encoder that includes one or more encryption stages. Each of the one or more encryption stages includes a non-linear substation module that includes a plurality of substitution boxes and each of the substitution boxes is configured to receive at least a subset of the control signal and subset of the set of data bits. Each substitution box substitutes a first output value for the subset of the set of data bits if the subset of the control signal is a first value, and substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value. *The second output value is formed such that a cryptographic weakness in the first out put value is at least partially compensated by a corresponding cryptographic strength in the second output value.*

Claims 3-12, 15-17, 19 and 20 are allowed because of dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100